

February 23, 2016

VIA ELECTRONIC FILING

Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

RE: **Annual 47 C.F.R. § 64.2009(c) CPNI Certification for 2015**
EB Docket No. 06-36
BAYCOM, INC
FCC 499 Filer ID: 821720 / FRN: 002-7153-08

I, Steven A. Elias, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures effective during the calendar year 2015 that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§ 64.2001-2011 of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement which (i) explains how the company's procedures ensure that the company is in compliance with the requirements set forth in section 47 C.F.R. §§ 64.2001 et seq. of the Commission's rules, (ii) explains any action taken against data brokers during the past year, (iii) reports information known to the company regarding tactics pretexters may be using to attempt access to CPNI, and (iv) summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI.



Name: Steven A Elias

Title: President

Date: February 23, 2015

BAYCOM, INC

CPNI Certification

499 Filer ID: 821720

FRN: 002-7153-08

STATEMENT

BAYCOM, ("Carrier") has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: None

BAACOM, INC.
CIVIL COMPLAINT
Case No. 1:13-cv-01130
Date Filed: 03/28/13

EXHIBIT

BAACOM ("Carrier") has established operating procedures that ensure compliance with the Federal Communications Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

* Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.

* Carrier has fully educated and trained its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI policies established by Carrier.

* Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined before any use of CPNI.

* Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customer's CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and the products and services were offered as part of the campaign.

* Carrier has established a supervisory review process regarding compliance with the CPNI rules that report to senior management. Carrier's sales personnel and supervisory personnel are trained on a regular basis regarding the CPNI rules. Carrier's sales personnel are trained on the CPNI rules and are required to follow the CPNI rules in all sales and marketing activities.

* Carrier has established procedures to notify law enforcement and customers of any unauthorized disclosure of CPNI in accordance with FCC directives.

* Carrier took the following actions against data brokers, including proceeds for inclusion in the Commission's state commission, in the event system or at the federal Communications Commission.

BAYCOM, INC

CPNI Certification

499 Filer ID: 821720

FRN: 002-7153-08

- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and [if any] what steps carriers are taking to protect CPNI: **Carrier has determined that no pretexter has attempted to access CPNI on Carriers System**

- The following is a summary of all customer complaints received in 2013 regarding the unauthorized release of CPNI:
 - Number of customer complaints Carrier received in 2013 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: **None**
 - Category of complaint:
 - 0 Number of instances of improper access by employees
 - 0 Number of instances of improper disclosure to individuals not authorized to receive the information
 - 0 Number of instances of improper access to online information by individuals not authorized to view the information
 - 0 Number of other instances of improper access or disclosure
 - Description of instances of improper access or disclosure: **None**

DAYCOM INC
CPI Certification
Case No: 251120
Ref: 002-1123-08

The following information Carter has with respect to the process & controls are used to ensure that no unauthorized access to CPI or related information is gained. Carter has taken steps to ensure that no unauthorized access to CPI or related information is gained.

The following is a summary of all customer complaints received in 2013 regarding the unauthorized access to CPI:

Number of customer complaints Carter received in 2013 related to unauthorized access to CPI or unauthorized disclosure of CPI: None

Category of complaint:

- o Number of instances of improper access by employees
- o Number of instances of improper disclosure to individuals not authorized to receive this information
- o Number of instances of improper access to online information by individuals not authorized to view this information
- o Number of other instances of improper access or disclosure: None
- o Description of instances of improper access or disclosure: None